UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924

7590 01/11/2006

Jack Friedman
SCHMEISER OLSEN and WATTS
3 Lear Jet Lane
Suite 201
Lathan, NY 12110

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/966,227	**Applicant(s)** BARDSLEY ET AL.	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-7,10-12 and 19-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-7,10-12 and 19-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 10/24/2005.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/20/2005 has been entered.

Response to Arguments

Applicant's arguments with respect to claim 5-7, 10-12, and 19-30 have been considered but are moot in view of the new ground(s) of rejection.

Claims 5-7, 10-12, and 19-30 have been examined, while claims .

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5-7, 10-12, and 19-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 5 and 10 recite the limitation "said denial of service attack" in line 4. There is insufficient antecedent basis for this limitation in the claim. The examiner will assume the limitation was meant to refer to the "denial of service intrusion".

Claims 19 and 25 recite the limitation "the protect device" in line 4. There is insufficient antecedent basis for this limitation in the claim. The examiner will assume the limitation was meant to refer to the "protected device".

Claims 6-7, 11-12, and 19-30 are rejected by virtue of their dependency to claims 5 and 10.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 5, 10, and 19-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US Patent Number 6,279,113), and further in view of Sharma et al. (US Patent Number 6,909,692) hereinafter referred to as Sharma

Regarding claim 5, Vaidya disclosed a method of operating an intrusion detection system, comprising the steps of: monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a DOS intrusion on a protected device, said DOS attack attempting to impede operation of the protected device (See Vaidya Abstract and Col. 12 Paragraphs 2-3); when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity (See Vaidya Col. 12 Lines 26-36); when the value of the signature event counter exceeds the signature threshold quantity, generating an alert by the intrusion detection sensor of the intrusion detection system (See Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6 Lines 20-26); but Vaidya failed to disclose recording a time for generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from the contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; or when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection system to decrease an alert generation rate of the intrusion detection system.

Sharma teaches that generating too many alerts in a network management system can crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8 Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and Col. 7 Lines 1-23).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate, and if greater than the threshold altering the attack signature profile to indicate a new threshold for event rate in order to begin transmitting alerts again. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the system administrator from being over informed as well as protecting the management system from crashing.

Regarding claim 10, Vaidya disclosed programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of: monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a DOS intrusion on a protected device, said DOS attack attempting to impede operation of the protected device (See Vaidya Abstract and Col. 12 Paragraphs 2-3); when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity (See Vaidya Col. 12 Lines 26-36); when the value of the signature event counter exceeds the signature threshold quantity, generating an alert by the intrusion detection sensor of the intrusion detection system (See Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6 Lines 20-26); but Vaidya failed to disclose recording a time for generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from the contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; or when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection system to decrease an alert generation rate of the intrusion detection system.

Sharma teaches that generating too many alerts in a network management system can crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8 Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See

Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and Col. 7 Lines 1-23).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate, and if greater than the threshold altering the attack signature profile to indicate a new threshold for event rate in order to begin transmitting alerts again. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the system administrator from being over informed as well as protecting the management system from crashing.

Regarding claims 19 and 25, Vaidya and Sharma disclosed alerting an administrator of suspected DOS intrusions upon the protected device (See Vaidya Col. 6 Lines 20-26).

Regarding claims 20 and 26, Vaidya and Sharma disclosed that the alert generation rate threshold is comprised by the governor (See Sharma Col. 9 Lines 16-26).

Regarding claims 21 and 27, Vaidya and Sharma disclosed that the signature set comprises a unique signature set identifier (See Vaidya Col. 10 Lines 25-45 “Pattern”), the signature event (See Vaidya Col. 10 Lines 25-45 “Attack_Signature”), the signature event counter (See Vaidya Col. 12 Paragraph 3 “counter”), the signature threshold quantity (See Vaidya Col. 12 Paragraph 3 “threshold”), and a signature threshold interval that specifies a sliding time window (See Vaidya Col. 12 Paragraph 3 “predetermined time interval”.

Regarding claims 22 and 28, Vaidya and Sharma disclosed that the protected device is selected from the group consisting of a computer, a web server, and a workstation (See Vaidya Col. 10 Lines 54-57).

Regarding claims 23 and 29, Vaidya and Sharma disclosed entering into the log a list of timestamps that record the times at which the intrusion detection sensor generates alerts, wherein said determining from contents of the log a present alert generation rate utilizes the timestamps in the log (See Sharma Col. 9 Paragraph 2).

Regarding claims 24 and 30, Vaidya and Sharma disclosed that after generating the alert and before determining from contents of the log the present alert generation rate, the method further comprises the step of: clearing the log of any entries that are past a specific age (See Sharma Col. 9 Paragraph 2 and Vaidya Col. 12 Paragraph 2 wherein Vaidya disclosed purging the expired entries of a log prior to determining the generation rate associated with the log).

Claims 6, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency of alert generation by halting the alert generation (See the rejection of claim 5 above), but failed to disclose altering the threshold quantity in order to do so.

Lunt teaches that alarms do not always pertain to individual events, and because they can come very quickly, after the first alarm is generated, subsequent alarms should be suppressed until a second threshold, greater than the first, is reached (See Lunt Page 14 Lines 11-17).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lunt in the alert generation system of Vaidya and Sharma, by suppressing alerts after the first threshold was reached, until a higher threshold is reached. This would have been obvious because the ordinary person skilled in the art would have recognized that multiple attacks can occur at the same time and would not want to ignore attacks after the first initial attack.

Claims 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further in view of Martin et al. (US Patent Number 6,772,349) hereinafter referred to as Martin.

Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency of alert generation by halting the alert generation (See the rejection of claim 5 above) and that the generation rate was determined using a sliding time window (See Vaidya Col. 12 Paragraph 2), but failed to disclose altering the threshold interval in order to do so.

Martin teaches that in a network intrusion detection system, the time interval used to collect signature data is indirectly proportional to the number of false alarms detected (See Martin Col. 5 Lines 30-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Martin in the alert suppressing system of Vaidya and Sharma, by decreasing the time interval once the threshold was broken. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that legitimate alerts were detected while false alarms were reduced.

Conclusion

Claims 5-7, 10-12, and 19-30 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU2131
1/5/06

Matthew Henning
Assistant Examiner
Art Unit 2131
12/29/2005